REMARKS

The Examiner is thanked for the careful review of this application.

Favorable reconsideration and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks. Claims 1-4, 6-8, 10-15, and 17-27 are pending in the current application. Claims 1, 10, 11, 18, and 19 are independent claims. Claims 26-27 are pending in the current application.

Reply to Office's Response to Arguments

Because the Office has maintained the prior rejections and has provided arguments in support of this position, and the Applicants will now address the Office's response to these arguments.

1. Regarding Section A of the Response to Arguments.

On Pages 15-16 of the Response to Arguments section, the Office explains that the claim language of "applications that do not comply with the predefined security protocol" is read upon applications in Bilange that are initially downloaded without an unlock code that is a prerequisite for their execution. Thus, the "predefined security protocol" is being read upon downloading applications with the unlock code. After establishing this interpretation of Bilange, the Office begins a discussion related to the MIDP as being executed by a Java application manager which the Office interprets as being "outside of the resident application environment." *Id.* The Applicants respectfully disagree with this interpretation of Bilange.

Firstly, an application being downloaded without the unlock code is not in violation of Bilange's security protocol. In Bilange, the unlock code controls the execution of an application; not its download. So, downloading an application without an unlock code in Bilange is not in violation of any security policy. Bilange states "the application provisioning server takes control of the registered application on first launch to get an unlock code that will be stored on the mobile device for subsequent launches" (e.g., [0046] of Bilange, Emphasis added) and "the license or unlock code is first fetched from the server as soon as the registered application is launched" (e.g., [0072] of Bilange, Emphasis added).

As will be appreciated, for an application to be launched on a mobile device, the application must already have been downloaded to the mobile device. Accordingly, all applications in Bilange are downloaded without the unlock code and the unlock code is then acquired from the server in conjunction with its first launch or execution as a condition for continued execution and/or subsequent executions. Thus, interpreting an application as being downloaded without the unlock code as in violation of a security policy in Bilange is incorrect, because the security policy is simply enforced during the first attempted launch of the application.

By contrast, in claim 1 as an example, applications are known to comply or not comply with the "predefined security protocol" when these applications are downloaded. Again, Bilange does not know whether an application is permitted to execute until the first launch of that application results in provisioning of the appropriate unlock code, which cannot be known when that application is downloaded.

Secondly, the Applicants believe that downloaded applications (in accordance with any security protocol) are only executed in one runtime environment in Bilange, namely, the J2ME environment. For example, the MIDP applications are subject to the same runtime environment as any other application, i.e., the J2ME runtime environment, and are subject to the same execution rules as any other application. As explained by Bilange at [0015], MIDP applications are simply MIDlets used in web browsers, but these applications are still "implemented in a J2ME environment."

The Office's statement that "[t]he application is loaded by the Java application manager this means the execution is outside of the resident application environment" (e.g., see Page 16 of the Office Action) is an incorrect conclusion to draw from Bilange's disclosure. Consider that Bilange states "[t]he MIDlet is the root of all MIDP applications and can be started, paused and stopped by the Java Application Manager on the device." (e.g., [0015] of Bilange). In context, the Java application manager executes within the J2ME runtime environment, and the Java application manager is responsible for both starting execution of some applications (with unlock codes, presumably) while stopping execution of other applications (those lacking unlock codes or for some other reason). In any case, in Bilange, only a single runtime environment is involved for any application that is actually permitted to execute.

Thirdly, in Bilange, the Applicants believe that applications that require an unlock code but do not yet have the unlock code are not permitted to execute at all. The Office has not cited to any example of an application in Bilange as lacking a required unlock code yet having been permitted to execute anyway. If it is the Office's contention that it is possible for an application to be launched first without having acquired the unlock code and allowed to be executed for a period of time without the unlock code, the Applicants submit that even in such an example, the application is forced to shut down by the Java application manager. Furthermore, even in such limited execution example, the same runtime environment is be used to execute the application irrespective of whether an unlock code has been obtained.

For at least these reasons, the Applicants respectfully submit that independent claims 1, 10-11, and 18-19 are allowable over Koskimies in view of Bilange.

2. Regarding Section B of the Response to Arguments.

In the 8/11/2011 Amendment, the Applicants argued against a very specific manner in which Hericourt is combined with Koskimies and Bilange. In particular, the Applicants argued that the unlock code from Bilange, which is related to copyright protection, would not be "borrowed" by Hericourt for use in an anti-virus scheme.

The Office appears to have misunderstood this argument because the Office mischaracterizes the Applicants' position as if the Applicants were arguing that a device could not protect against viruses and copyright infringers at the same time. This was not the point that the Applicants were trying to make. Rather, the Applicants' point was that the Office is trying to mishmash a copyright protection scheme and an anti-virus scheme together in a manner that does not make sense.

As noted in the previous section, whether an application is in compliance with the claimed "predefined security protocol" is read upon Bilange as the presence or absence of the unlock code. The unlock code permits execution for applications that are confirmed by a server to be authorized for execution at the target device. This has absolutely nothing to do with device protection against viruses.

Claim 25 recites "wherein the predefined security protocol is configured to protect the computer device," which is not read upon the presence or absence of the unlock code in Bilange. The Office cites to Hericourt for curing this deficiency but, in doing so, the Office is no longer factoring in claim 25 "as a whole". Hericourt is directed to device protection against viruses, but Hericourt provides no rationale for specifically implementing its virus protection by blocking applications from execution based on the unlock code from Bilange. Without such a teaching, Hericourt simply motivates one of ordinary skill in the art to implement a parallel virus protection system on top of Bilange's copyright protection system, not to merge these different protection systems into a hybrid system.

Accordingly, because the Office reads the claimed "predefined security protocol" upon Bilange's disclosure related to the unlock code, the Office's citation to Hericourt as a mere example of a device protection system is insufficient to motivate one of ordinary skill in the art to modify Bilange so that the unlock code itself is used in a fundamentally different manner.

3. Allowance Requested for Newly Added Claims 26-27.

Claim 26 recites "wherein compliance with the predefined security protocol for a given application is based upon information contained with the given application during download and prior to execution of the given application", and is supported at least by "if the application sought downloaded does not comply with a predefined security protocol, such as the verification of a certificate present in the download" (e.g., [0019] of the published Specification). As already discussed above, the unlock code in Bilange is only obtained after an application is already downloaded and launches for the first time. As such, the unlock code cannot be said to be present at the time of download prior to the application's execution.

Claim 27 clarifies that the "download manager" downloads a non-compliant application after an initial attempt and refusal to download the non-compliant application by the "resident application environment. For example, "if the application sought downloaded does not comply with a predefined security protocol … the resident application environment will refuse to download the unverifiable application. The end-user of the wireless device 10 can also selectively attempt download non-security protocol complying applications" (e.g., see [0019] of the published Specification), whereby "[t]o allow the download and/or execution of the unverified/non-complying application, the present wireless device platform 12 includes a download manager 18 that can handle the unverified application partially or fully independently of the resident application environment" (e.g., [0023] of the published Specification). The Java download manager in Bilange appears to handle the download of any application irrespective of whether the applications, once downloaded, can successfully obtain an unlock code upon launch.

SUMMARY

Since the Office has maintained the rejections of claims 1-4, 6-8, 10-15 and 17-25 under 35 U.S.C. § 103(a) as noted above, the Applicants once again traverse these rejections. The Applicants expressly maintain the reasons from the prior responses to clearly indicate on the record that the Applicants have not conceded any of the previous positions relative to the maintained rejections. For brevity, the Applicants expressly incorporate the prior arguments presented in the 8/11/2011 response without a literal rendition of those arguments in this response.

For at least the foregoing reasons and the reasons set forth in Applicants' response of 8/11/2011, it is respectfully submitted that claims 1, 10, 11, 18, and 19 are distinguishable over the applied art. The remaining dependent claims are allowable at least by virtue of their dependency on the above-identified independent claims. See MPEP § 2143.01. Moreover, these claims recite additional subject matter, which is not suggested by the documents taken either alone or in combination.

CONCLUSION

In light of the remarks and/or amendments contained herein, the Applicants respectfully submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: December 20, 2011

By: /Fariba Yadegar-Bandari/

Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502